**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G07F 7/10 — A1

(11) International Publication Number: WO 93/24906

(43) International Publication Date: 9 December 1993 (09.12.93)

(21) International Application Number: PCT/US93/05357

(22) International Filing Date: 4 June 1993 (04.06.93)

(30) Priority data:
07/893,670 4 June 1992 (04.06.92) US

(71) Applicant: INTEGRATED TECHNOLOGIES OF AMERICA, INC. [US/US]; 610 11th Avenue South, Hopkins, MN 55343 (US).

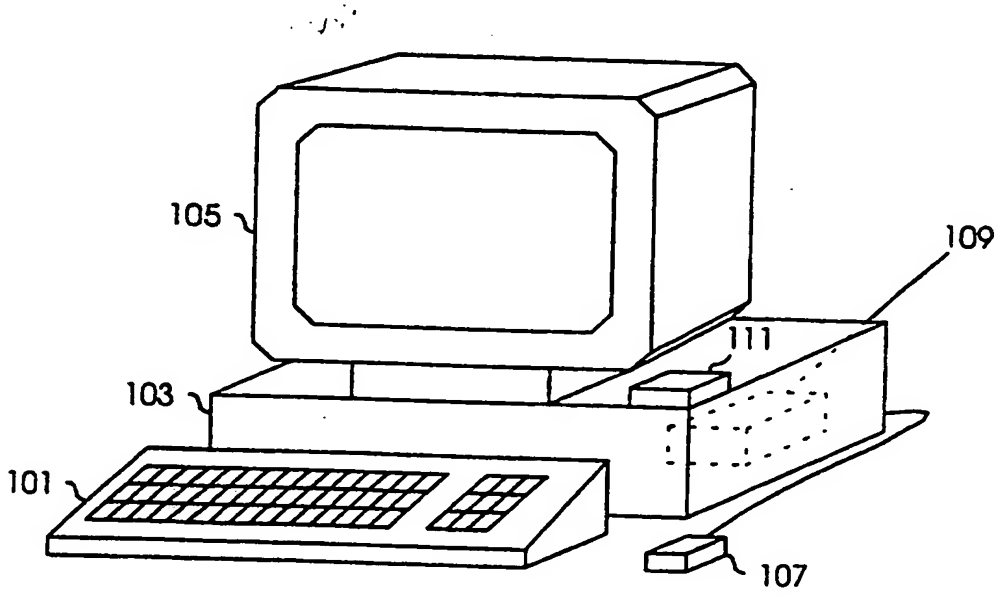
(72) Inventors: MOONEY, David, M. ; 8938 Hidden Oaks Drive, Eden Prairie, MN 55344 (US). GLAZIER, James, B. ; 1020 Feltl Courts, #306, Hopkins, MN 55343 (US). WOOD, David, E. ; 5385 Wedgewood Drive, Shorewood, MN 55331 (US). KIMLINGER, Joseph, A. ; 307 Warner Road, Willernie, MN 55090 (US). GOSHGARIAN, Paul ; 5965 Lakeview Drive, Mound, MN 55364 (US).

(74) Agent: BRUESS, Steven, C.; Merchant, Gould, Smith, Edell, Welter & Schmidt, 3100 Norwest Center, 90 South Seventh Street, Minneapolis, MN 55402 (US).

(81) Designated States: AU, BR, CA, JP, KR, RU, UA, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

**Published**
*With international search report.*
*Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.*

(54) Title: PROTECTING PROGRAMS AND DATA WITH CARD READER




(57) Abstract

A secure computer controlling access to internal devices via an integrated card reader. A microprocessor-controlled card reader interface logically connected to the CPU of the computer reads and writes information from and to a card placed in the card reader and performs additional functions in response to commands received from the CPU. The boot ROM of the computer is programmed to start execution from a program logic device which runs a verification program to verify the authenticity of a user. Upon a valid user card being placed in the card reader, one or more questions are read from the card and displayed to the user. The user's responses are saved and compared to the correct answers stored on the card, and if the responses match the correct answers, a power control circuit is used by the CPU to turn on power to computer peripherals the user has been authorized to use.

*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | |
|---|---|---|---|---|---|
| AT | Austria | FR | France | MR | Mauritania |
| AU | Australia | GA | Gabon | MW | Malawi |
| BB | Barbados | GB | United Kingdom | NL | Netherlands |
| BE | Belgium | GN | Guinea | NO | Norway |
| BF | Burkina Faso | GR | Greece | NZ | New Zealand |
| BG | Bulgaria | HU | Hungary | PL | Poland |
| BJ | Benin | IE | Ireland | PT | Portugal |
| BR | Brazil | IT | Italy | RO | Romania |
| CA | Canada | JP | Japan | RU | Russian Federation |
| CF | Central African Republic | KP | Democratic People's Republic of Korea | SD | Sudan |
| CG | Congo | | | SE | Sweden |
| CH | Switzerland | KR | Republic of Korea | SK | Slovak Republic |
| CI | Côte d'Ivoire | KZ | Kazakhstan | SN | Senegal |
| CM | Cameroon | LI | Liechtenstein | SU | Soviet Union |
| CS | Czechoslovakia | LK | Sri Lanka | TD | Chad |
| CZ | Czech Republic | LU | Luxembourg | TG | Togo |
| DE | Germany | MC | Monaco | UA | Ukraine |
| DK | Denmark | MG | Madagascar | US | United States of America |
| ES | Spain | ML | Mali | VN | Viet Nam |
| FI | Finland | MN | Mongolia | | |

# PROTECTING PROGRAMS AND DATA WITH CARD READER

## Field of the Invention

The present invention pertains generally to integrated circuit (IC) information card systems, and more particularly to a microprocessor-controlled card reader interface for controlling user access to the components of a secure computer.

## Background of the Invention

The power and flexibility of personal computers has seen a tremendous growth in their use in all areas of our society, including applications where the data is sensitive in nature. Traditionally, these applications have been found within agencies of the federal government, but the highly competitive marketplace has made such information as marketing, financial, and business plans equally as sensitive to companies who compete against each other in the commercial sector as well.

In the early years of the industry when computers were large mainframes, it was relatively easy to control access to them simply by controlling physical access to the room they were contained in. Since modern personal computers are much smaller and may in fact be designed to be carried with a user, it is much more difficult to prevent unauthorized access while still maintaining the advantage of portability.

While it is possible through a software program running on the computer to require a user to enter a password or other verification code, this method is not robust in that a password may be guessed, or the software program may be bypassed by commercially available software development tools. Other security methods involving various hardware devices or keys have been proposed and implemented, but they too suffer from the disadvantage that a sufficiently knowledgeable and persistent user may gain unauthorized access to data by tapping into the computer's operating system with specially designed software programs. For applications

with particularly sensitive data, it may also be desirable to provide a way to physically and logically destroy the data before it becomes compromised.

Therefore, there is a need to have a convenient way to prevent the unauthorized use of a computer system which is not subject to bypass while still maintaining the portability and flexibility of the computer system. There is an additional need to provide a way to authorize users to use the computer system. There is a further need to physically and logically destroy data in response to unauthorized attempts by a user to violate the physical or logical integrity of the computer system.

## Summary of the Invention

The present invention provides for a secure computer controlling access to internal devices via an integrated card reader. A microprocessor-controlled card reader interface logically connected to the CPU of the computer reads and writes information from and to a card placed in the card reader and performs additional functions in response to commands received from the CPU. The boot ROM of the computer is programmed to start execution from a program logic device which runs a verification program to verify the authenticity of a user. Upon a valid user card being placed in the card reader, one or more questions are read from the card and displayed to the user. The user's responses are saved and compared to the correct answers stored on the card, and if the responses match the correct answers, a power control circuit is used by the CPU to turn on power to computer peripherals the user has been authorized to use.

According to an additional aspect of this invention, the system provides for a method of initializing and authorizing a user card with a security administrator card. Upon a valid security administrator card being placed in the card reader, a security

administrator initializes and authorizes one or more individual user cards by selecting from a list of menu options displayed to the security administrator. The security administrator inputs a list of questions and answers which are then stored on the user card for use during the verification procedure.

According to a further aspect of this invention, the system provides for the physical and logical destruction of data in response to unauthorized attempts by a user to violate the physical or logical integrity of the computer system. The physical and logical destruction of data may be disabled for maintenance or configuration purposes by the use of a maintenance card.

The preceding and other features and advantages of the invention will become further apparent from the detailed description that follows. This description is accompanied by a set of drawing figures. Numerals are employed throughout the written description and the drawings to point out the various features of this invention, like numerals referring to like features throughout.

## Brief Description of the Drawings

Figure 1 is a perspective view of a secure computer system according to the present invention.

Figure 2 is a block diagram showing the high-level architecture of a secure computer system according to the present invention.

Figure 3 is a schematic diagram showing the microprocessor-controlled card reader interface for a secure computer system according to the present invention.

Figure 4 is a flow diagram showing the steps taken to read and write information from and to a card according to the present invention.

Figure 5 is a flow diagram showing the steps taken to verify a user according to the present invention.

Figure 6 is a flow diagram showing the steps taken to authorize a user according to the present invention.

Figure 7 is a flow diagram showing the steps taken to deactivate the physical and logical destruction of data according to the present invention.

## Detailed Description of the Preferred Embodiments

In the following detailed description of the preferred embodiments, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

The following is a list of reference numerals and descriptions corresponding to the numerals employed in the accompanying set of drawing figures.

**NUMERALS AND DESCRIPTIONS**

| | |
|---|---|
| 101 | keyboard |
| 103 | computer chassis |
| 105 | screen display |
| 107 | pointing device |
| 109 | card reader interface |
| 111 | integrated card reader |
| 113 | integrated circuit (IC) card |
| 115 | microprocessor |
| 117 | second data bus |
| 119 | power control circuit |
| 121 | peripheral devices |
| 123 | central processing unit (CPU) |
| 125 | system data bus |
| 126 | boot rom |
| 127 | random access memory (RAM) |
| 129 | program logic device (PLD) |
| 131 | third data bus |
| 133 | fourth data bus |
| 135 | power circuit |
| 137 | clear |
| 139 | +5 volt lithium battery |

141 address or data select
143 strobe
145 chip select
147 clear to send (CTS)
149 data terminal ready (DTR)
151 10 MHz clock
153 serial data out
155 serial data in
157 3.5 MHz clock
159 card reset
161 card serial data control
163 card interrupt control
165 physical destruct
167 card serial data in
169 card serial data out
171 card power control switch
173 card power control line
175 +5 volt relay
177 card serial data contact
179 card clock contact
181 card reset contact
183 card logic voltage supply contact
185 card ground contact
187 card programming contact
189 card detect contact
191 card detect power contact
193 reserved for future use
195 reserved for future use
197 reserved for future use

**DETAILED DESCRIPTION**

Figure 1 shows the components of a computer system to be secured with a card reader interface. The computer system includes a keyboard 101 by which a user may input data into the system, a computer chassis 103 which holds electrical components and peripherals, a screen display 105 by which information is displayed to the user, and a pointing device 107, the system components logically connected to each other via the internal system bus of the computer. A card reader 111 is connected to the secure computer system via card reader interface 109. The preferred card reader 111 is an Amphenol® "Chipcard" acceptor device, part number C 702 10 M 008 103 4, which is compatible with International Standards Organization (ISO) specification 7816, although one skilled in the art would readily recognize that other card reader devices which conform to ISO 7816 may be substituted.

In order for the computer system to be secured, a card reader interface is integrated into the computer system in a manner similar to that as revealed in Figure 2. A card reader interface board 109 contains a microprocessor 115 connected to the CPU of the computer via a second data bus 117, connected to RAM 127 via a third data bus 131, and connected to the card reader 111 via a fourth data bus 133. The interface board 109 is typically implemented with printed circuit board technology, although other equivalent technologies may be substituted without loss of generality. Peripherals 121 within computer 103 are controlled by the CPU 123 and PLD 129 with a power control circuit 119, which turns power off and on to peripherals 121. A system boot ROM 126 logically connected to the CPU 123 via system data bus 125 is programmed to instruct the CPU 123 to start executing a non-volatile program contained in PLD 129 upon power-up, clear, or warm-boot reset of the computer.

An IC card 113 is used in conjunction with card reader 111. The preferred IC card 113 is a MICRO CARD® model SCOT 100 or model TB100 IC card, which is compatible with ISO standards 7810, 7813, and 7816. By conforming to these standards, the IC card 113 provides support for Data Encryption Standard (DES) data encryption and decryption functions. One skilled in the art would readily recognize that other IC cards which conform to these standards and provide data encryption and decryption functions may be substituted. The ability to encrypt and decrypt data is important, since the present invention is designed to never allow unencrypted security data to exist on the CPU where it could be subject to compromise by a malicious user.

The schematic for card reader interface 109 is described in greater detail in Figure 3. Microprocessor 115 is powered by circuit 135, and controls system functions via connections to the system data bus 125.

System resets are initiated by clear line 137. Validation and authorization information is transferred between the microprocessor 115 and RAM 127 via the third data bus 131 in conjunction with address or data select line 141, strobe line 143, and chip select line 145. Backup power is provided for RAM 127 by a +5 volt lithium battery 139.

The microprocessor 115 communicates with system data bus 125 as a serial communications device using CTS line 147, DTR line 149, 10 MHz clock line 151, serial data out line 153, and serial data in line 155. A separate 3.5 MHz clock line 157 is used to provide a clock signal to PLD 129, which is used by the microprocessor 115 for card reset control via line 159, card serial data control via line 161, and card interrupt control via line 163. The PLD 129 in turn connects to the card via card serial data contact 177, card clock contact 179, and card reset contact 181. The microprocessor 115 also has the ability to control the physical destruction of data within the computer system via line 165. The line connects to a machanism containing a chemical solution which is sprayed onto a hard disk contained in the secure computer system in response to unauthorized attempts by a user to violate the physical or logical integrity of the computer system. The preferred chemical solution is that of ferric chloride, however, one of ordinary skill in the art would recognize that other equivalent destruction chemicals and mechanisms may be substituted without loss of generality.

The microprocessor 115 uses power control line 173 with switch 171 and +5 volt relay 175 to provide power to the card via card logic voltage supply contact 183 and card programming contact 187. The card is grounded via card ground contact 185, and detected by power being applied through card detect power contact 191 to microprocessor 115 by card detect contact 189.

Card contacts 193 and 195 and line 197 are reserved for future use.

As illustrated by the method of Figure 4, the microprocessor 115 works in conjunction with CPU 123 running under program control of the PLD 129 in order to perform functions involving the card 113. The microprocessor 115 runs in an infinite loop interpreting and performing commands sent to it by the CPU 123. At 201, the microprocessor 115 is started by either a computer system power-up, a system clear, or a system warm-boot. At 203, a hardware interrupt is asserted on the system bus, the current status is sent to the CPU at 205, and at 207 the microprocessor 115 waits for a command to be received from the CPU 113. Upon receipt of a valid command 211, the command is processed at 209 and control returns to 207. The list of valid commands interpreted by the microprocessor 115 includes but is not limited to:

1. Clear
2. Card Power On
3. Card Power Off
4. Write Validation
5. Read Card
6. Read Card Encrypted
7. Write Card
8. Write Card Encrypted
9. Erase Card
10. Remove Card - No Clear
11. Wake-Up Call

Figure 5 shows the steps taken by the CPU 123 and microprocessor 115 in order to verify the authenticity of a user of the secure computer system. At 213, the microprocessor waits for a valid user card to be inserted into the card reader, and at 215 the CPU waits for the microprocessor to send a card type status code. If no card type is received, control returns to 213. If at 215 a card type is received, it is checked for validity at 217. If the card type is invalid, a status message is displayed to the user at 219 and control returns to 213. If at 217 the card type is valid, a question is read from the card at 221,

displayed to the user at 223, and the CPU waits for a user response at 225. Once the CPU receives a response from the user, the response is sent to the microprocessor at 227. The microprocessor compares the user response to the correct response stored on the card, and returns a compare status to the CPU at 229. This step is performed solely by the microprocessor so that unencrypted security data is never available to the CPU. If at 231 the compare status indicates a non-matching response, a retry counter is incremented at 233 and checked at 235 to see if it is less than a predetermined maximum allowed value. If the value of the retry counter is less than the maximum allowed value, control returns to 225, otherwise the secure computer system is rebooted at 237. If at 231 the compare status indicates a matching response, at 239 the CPU uses power control circuit 119 to turn on power to the secure computer system peripherals that the user has been authorized to use. Such peripherals might include, but are not limited to, a floppy disk drive, a hard disk drive, serial port, parallel port, and internal modem depending on the configuration of the secure computer system.

In an alternative embodiment, access to specific directories on a hard disk is enabled by IC card 113. A DES encryption chip attached to system data bus 125 is used with a modified version of the secure computer system basic input/output system (BIOS) to encrypt the information and files stored in a specific subdirectory with a key value. The key value for each subdirectory the user has access to is stored on the IC card 113. Upon successfully completing the verification procedure described above and shown in Figure 5, the key values for the subdirectories are read from the IC card 113 and used by the BIOS and DES chip to encrypt and decrypt information and files as needed by the user. If directory creation is allowed for the user, a personal

user key is used to encrypt and decrypt the new directory and all information and files contained within it.

The procedure used by a security administrator to authorize a user is revealed in Figure 6. At 241, the microprocessor waits for a valid administrator card to be inserted into the card reader, and at 243 the CPU waits for the microprocessor to send a card type status code. If no card type is received, control returns to 241. If at 243 a card type is received, it is checked for validity at 245. If the card type is invalid, a status message is displayed to the operator at 247 and control returns to 241. If at 245 the card type is valid, an authorization code is read from the card at 249, the operator is prompted for the code at 251, and the CPU waits for an operator response at 253. Once the CPU receives a response from the operator, the response is sent to the microprocessor and compared with the authorization code at 255. If at 257 the compare status indicates a non-matching response, a retry counter is incremented at 259 and checked at 261 to see if it is less than a predetermined maximum allowed value. If the value of the retry counter is less than the maximum allowed value, control returns to 253, otherwise the secure computer system is rebooted at 263. If at 257 the compare status indicates a matching response, at 265 the CPU waits for the administration card to be removed, displays a list of menu options to the operator at 267, and waits for an operator selection at 269.

The list of menu options includes but is not limited to exit, initialize card, and process security. If at 269 the operator selects exit, the program terminates and no further action is taken. If at 269 the operator selects initialize card, at 289 the CPU waits for a valid administrator card to be inserted into the card reader, gets an authorization code from the card at 291, and compares the code to an operator

response at 293. If at 295 the code matches the response, the operator is prompted to insert a valid user card at 297, and the user card is initialized at 299, otherwise control continues at 301. At 301 the operator is prompted to remove the card and the CPU then waits at 303 for the card to be removed. If at 305 there are no more cards to be initialized, control returns to 269, otherwise control returns to 289.

If at 269 the operator selects process security, at 271 the CPU waits for a valid administrator card to be inserted into the card reader, gets an authorization code from the card at 273, and compares the code to an operator response at 275. If at 277 the code does not match the response, control continues at 301. Otherwise, the operator is prompted to enter a list of questions and answers at 279, the CPU waits for an operator response at 281, then prompts the operator for the user card at 283. At 285 the user card is erased, the questions and answers and other information is written to the card at 287, and control continues at 301.

The secure computer system physically and logically destroys data within the system in response to unauthorized attempts by a user to violate the physical or logical integrity of the computer system. In order to deactivate this system in order to perform system maintenance or change the system configuration, a maintenance card is used with the procedure described in Figure 7. At 307 the CPU waits for a valid administrator card to be inserted into the card reader, gets an authorization code from the card at 309, and compares the code to an operator response at 311. If at 313 the code does not match the response, control returns to 307. Otherwise, upon detecting a valid maintenance card at 315, at 317 the CPU disables the physical destruction of data and clears RAM 127, then reboots the system at 319. The system may now be safety

shut down for maintenance. Physical and logical destruction of data are automatically reenabled upon the next time the system is restarted after maintenance or configuration is performed.

It is to be understood, however, that even though numerous characteristics and advantages of the invention have been set forth in the foregoing description, together with details of the structure and function of the invention, the disclosure is illustrative only, and changes may be made in detail, especially in matters of shape, size, and arrangement of parts within the principles of the invention, to the full extent indicated by the broad general meaning of the terms in which the appended claims are expressed.

**WHAT IS CLAIMED:**

1. A secure computer providing for the controlled access of internal devices via an integrated card reader, the computer comprising:

a user input device;

an integrated card reader;

a screen display;

a central processing unit (CPU);

a program logic device (PLD) containing non-volatile CPU program code;

a CPU system boot from the PLD;

a plurality of peripheral devices;

a system data bus;

a microprocessor for writing and reading information to and from a card placed in the card reader;

a second data bus logically connected between the microprocessor and the CPU and separate from the system data bus; and

a power control circuit logically connected between the CPU and each of the plurality of peripheral devices for selectively controlling power to each of the plurality of peripheral devices in response to information read from the card.

2. A secure computer providing for the controlled access of internal devices via an integrated card reader, the computer comprising:

a user input device;

an integrated card reader;

a screen display;

a central processing unit (CPU);

a program logic device (PLD) containing non-volatile CPU program code;

a CPU system boot from the PLD;

a plurality of peripheral devices;

a system data bus;

a microprocessor for writing and reading information to and from a card placed in the card reader;

a second data bus logically connected between the microprocessor and the CPU and separate from the system data bus;

a power control circuit logically connected between the CPU and each of the plurality of peripheral devices for selectively controlling power to each of the plurality of peripheral devices in response to information read from the card; and

means operative to cause said CPU to perform the step of:

waiting for a valid card to be placed in the card reader by the user;

reading at least one question from a list of questions stored on the card, displaying the question to the user on the screen display, and waiting for a response from the user on the input device;

comparing at least one user response to a list of correct answers stored on the card; and

allowing access to the computer if at least one user response matches a corresponding correct answer.

3. The computer of claim 2 wherein the CPU performs the additional step of incrementing the value of a retry counter if the user incorrectly answers a question, and waiting for a subsequent user response if the value of the retry counter is less than a predetermined value, otherwise rebooting the computer.

4. A secure computer providing for the controlled access of internal devices via an integrated card reader, the computer comprising:

a user input device;

an integrated card reader;

a screen display;

a central processing unit (CPU);

a program logic device (PLD) containing non-volatile CPU program code;

a CPU system boot from the PLD;

a plurality of peripheral devices;

a system data bus;

a microprocessor for writing and reading information to and from a card placed in the card reader;

a second data bus logically connected between the microprocessor and the CPU and separate from the system data bus; and

a power control circuit logically connected between the CPU and each of the plurality of peripheral devices for selectively controlling power to each of the plurality of peripheral devices in response to information read from the card.

program control means operative to cause the CPU to perform the authorization steps of:

waiting for a valid security administrator card to be placed in the card reader by an operator;

reading at least one authorization code from the security administrator card, prompting the operator for the authorization code, and waiting for a response from the operator;

comparing at least one operator response to the authorization code read from the card;

prompting the operator to remove the valid security administrator card and waiting for the card to be removed if all operator responses match a corresponding authorization code;

displaying a list of options to the operator via a main menu, prompting the operator to select an option, and waiting for a response from the operator; and

performing the function corresponding to the option selected from the main menu by the operator and

returning control back to the main menu.

5. The computer of claim 4 wherein the list of options comprises exit, initialize secure card, and process security.

6. The computer of claim 4 wherein if the operator selects exit, the authorization steps terminate with no further steps performed.

7. The computer of claim 4 wherein the program control means includes means operative when the operator selects initialize secure card to cause the CPU to perform the additional authorization steps of:

prompting the operator to insert a valid user card and waiting for a valid user card to be inserted;

reading at least one authorization code from the user card, comparing the card authorization code to the operator authorization code, and if the card has been previously used and the authorization codes do not match:

(i) prompting the operator to remove the user card and waiting for the card to be removed;

(ii) returning control back to the main menu;

erasing any information previously stored on the user card and writing the operator authorization code to the card; and

prompting the operator to remove the user card, waiting for the card to be removed, and returning control back to the main menu.

8. The computer of claim 4 wherein the program control means includes means operative when the operator selects process security to cause the CPU to perform the additional authorization steps of:

prompting the operator to insert a valid user card and waiting for a valid user card to be inserted;

reading at least one authorization code from the user card, comparing the card authorization code to the operator authorization code, and if the authorization codes do not match:

(i) prompting the operator to remove the user card and waiting for the card to be removed;

(ii) returning control back to the main menu;

prompting the operator for questions to ask the user and answers to the questions, and waiting for a response from the operator to all prompts;

erasing any information previously stored on the user card and writing the operator authorization code, questions, and answers to the card; and

prompting the operator to remove the user card, waiting for the card to be removed, and returning control back to the main menu if there are no more user cards to be authorized, otherwise looping until all remaining user cards are authorized.

9. A secure computer comprising:

a user input device;

an card reader;

a screen display;

a microprocessor for reading information from a card placed in the card reader; and

a circuit to control the operation of said computer to prevent unauthorized access.

10. A method of controlling access to a computer including

a user input device,

an card reader,

a screen display and

a microprocessor for reading information from a card placed in the card reader, the method comprising the step of:

reading information from the card and using it to prevent unauthorized access to the computer.

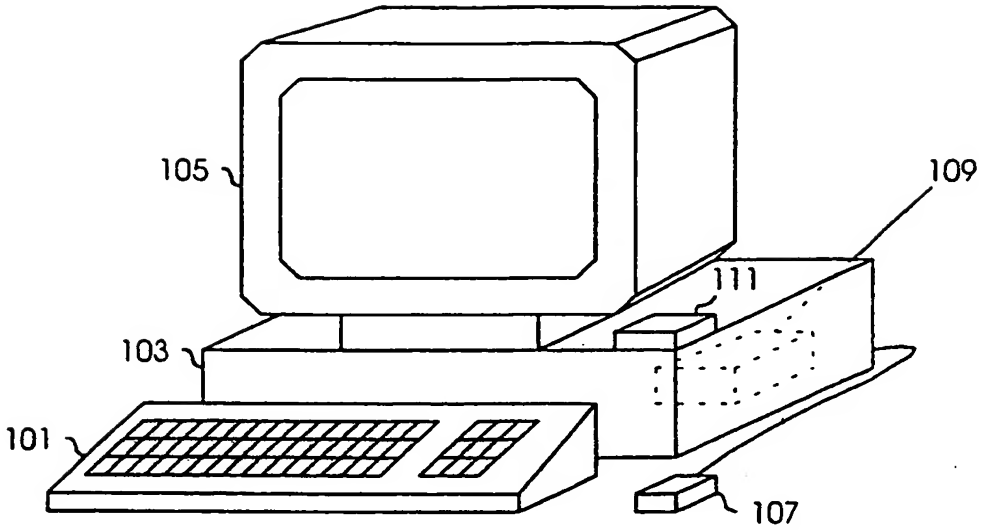

105
109
111
103
101
107

*Fig. 1*

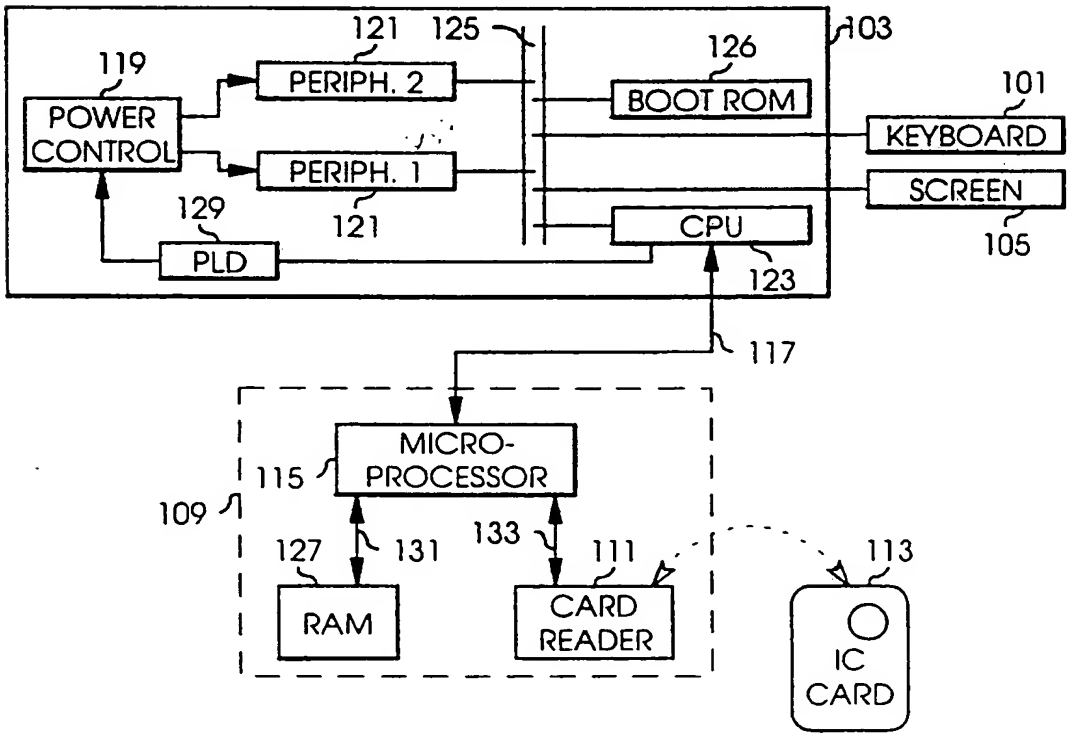

121
125
103
119
126
PERIPH. 2
BOOT ROM
101
POWER CONTROL
KEYBOARD
PERIPH. 1
SCREEN
129
121
CPU
105
PLD
123
117
MICRO-PROCESSOR
115
109
127
131
133
111
113
RAM
CARD READER
IC CARD

*Fig. 2*

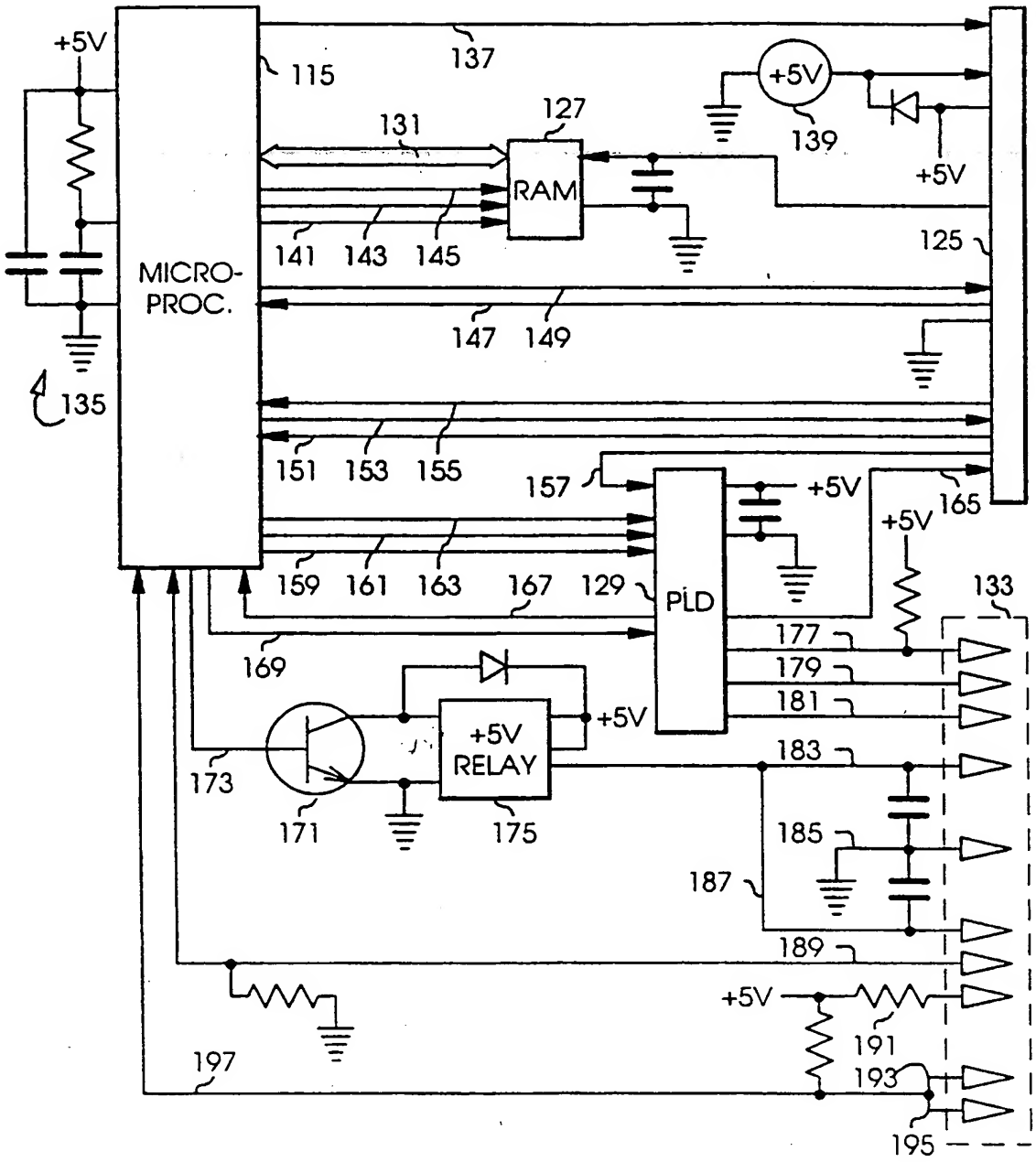

+5V
115
137
+5V
139
127
131
RAM
+5V
141
143
145
125
MICRO-
PROC.
147
149
135
151
153
155
157
+5V
165
+5V
159
161
163
167
129
PLD
133
177
169
179
181
+5V
+5V
RELAY
183
173
171
175
185
187
189
+5V
191
193
197
195

*Fig. 3*

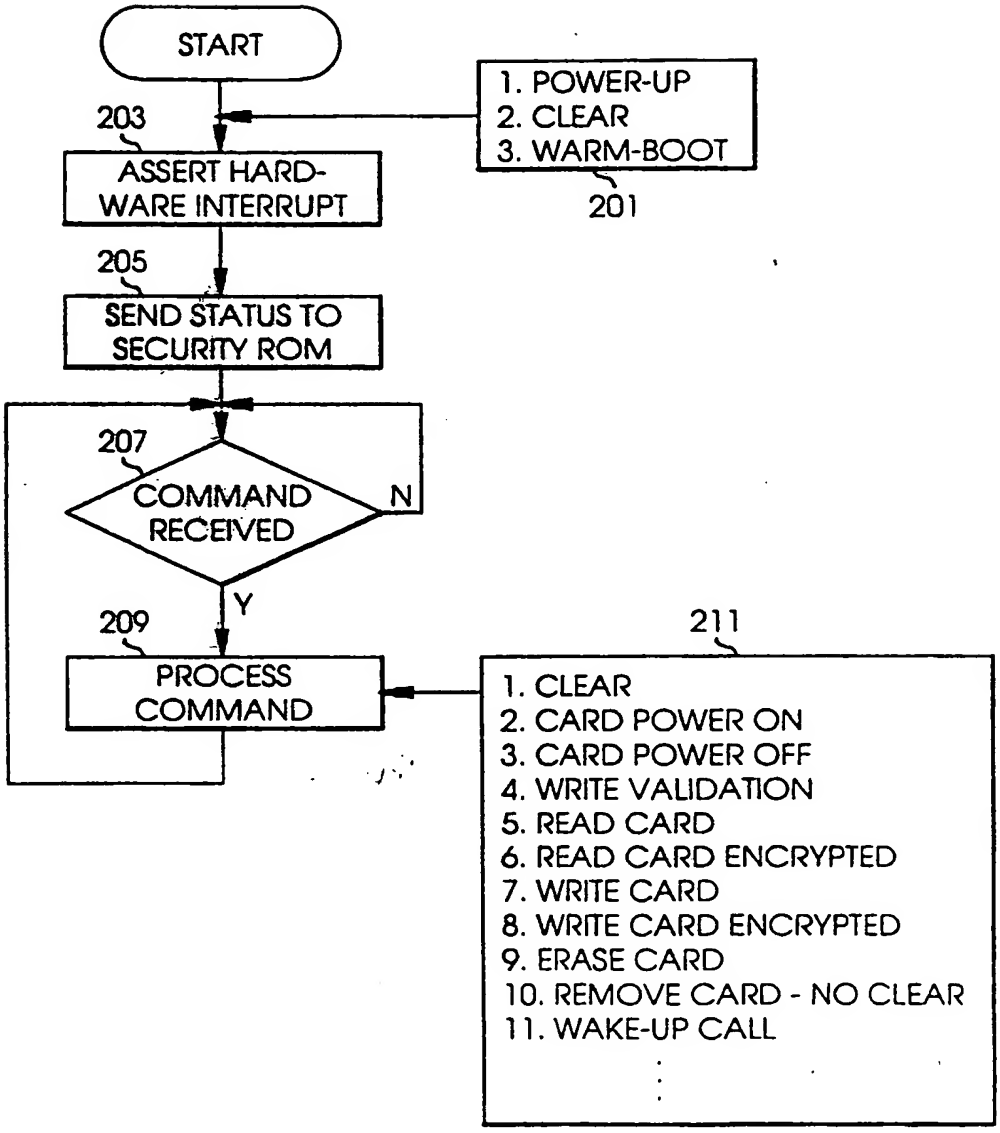

START
1. POWER-UP
2. CLEAR
3. WARM-BOOT
201
203
ASSERT HARD-WARE INTERRUPT
205
SEND STATUS TO SECURITY ROM
207
COMMAND RECEIVED
N
Y
209
PROCESS COMMAND
211
1. CLEAR
2. CARD POWER ON
3. CARD POWER OFF
4. WRITE VALIDATION
5. READ CARD
6. READ CARD ENCRYPTED
7. WRITE CARD
8. WRITE CARD ENCRYPTED
9. ERASE CARD
10. REMOVE CARD - NO CLEAR
11. WAKE-UP CALL

*Fig. 4*

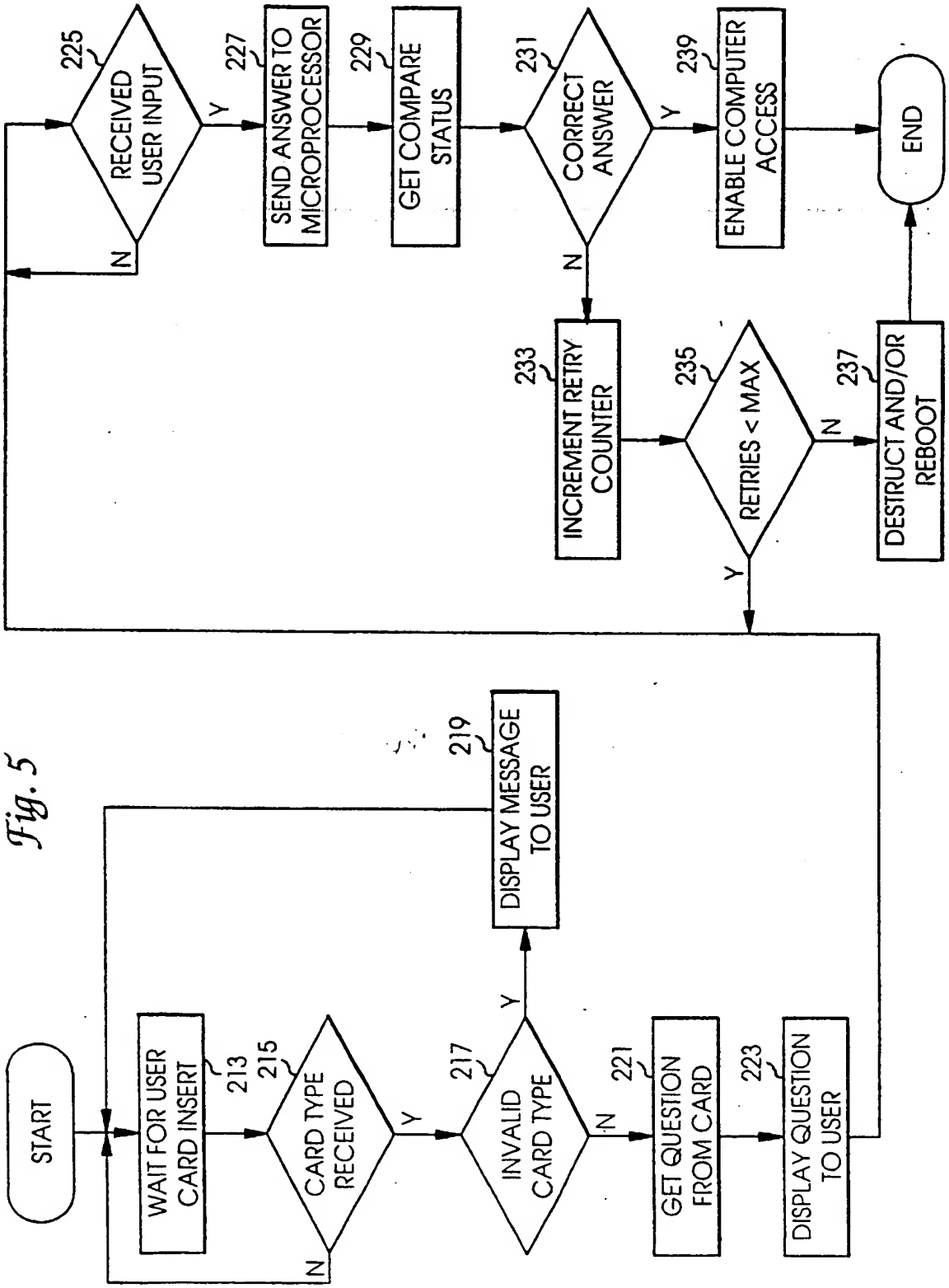

START
WAIT FOR USER CARD INSERT
213
CARD TYPE RECEIVED
215
N
Y
INVALID CARD TYPE
217
Y
N
DISPLAY MESSAGE TO USER
219
GET QUESTION FROM CARD
221
DISPLAY QUESTION TO USER
223
RECEIVED USER INPUT
225
N
Y
SEND ANSWER TO MICROPROCESSOR
227
GET COMPARE STATUS
229
CORRECT ANSWER
231
N
Y
INCREMENT RETRY COUNTER
233
RETRIES < MAX
235
Y
N
DESTRUCT AND/OR REBOOT
237
ENABLE COMPUTER ACCESS
239
END

*Fig. 5*

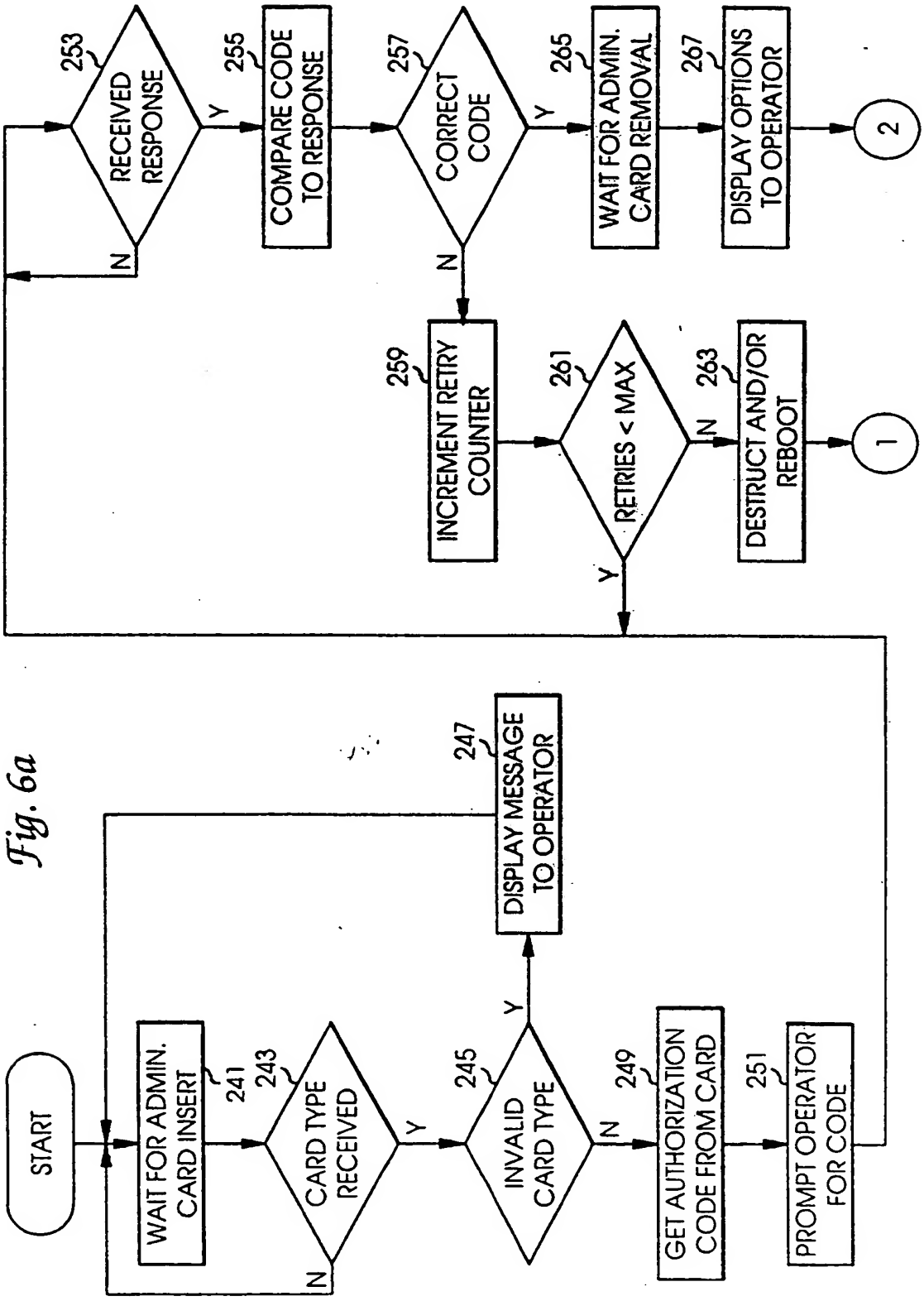
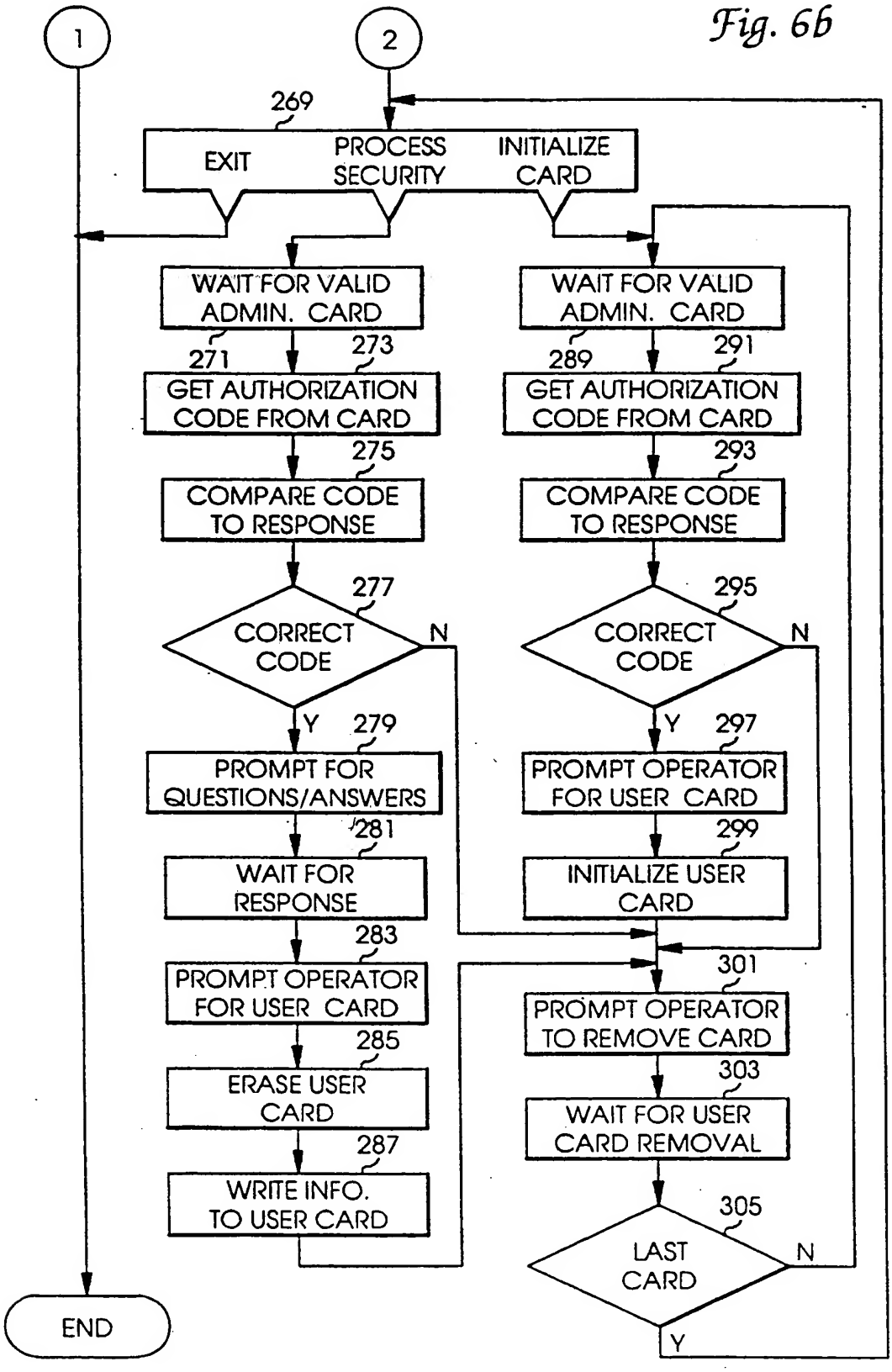

START
WAIT FOR ADMIN. CARD INSERT
241
CARD TYPE RECEIVED
243
N
Y
INVALID CARD TYPE
245
Y
N
DISPLAY MESSAGE TO OPERATOR
247
GET AUTHORIZATION CODE FROM CARD
249
PROMPT OPERATOR FOR CODE
251
RECEIVED RESPONSE
253
N
Y
COMPARE CODE TO RESPONSE
255
CORRECT CODE
257
N
Y
INCREMENT RETRY COUNTER
259
RETRIES < MAX
261
N
Y
DESTRUCT AND/OR REBOOT
263
WAIT FOR ADMIN. CARD REMOVAL
265
DISPLAY OPTIONS TO OPERATOR
267
1
2

Fig. 6a

Fig. 6b


1
2
269
EXIT
PROCESS SECURITY
INITIALIZE CARD
WAIT FOR VALID ADMIN. CARD
271
273
GET AUTHORIZATION CODE FROM CARD
275
COMPARE CODE TO RESPONSE
277
CORRECT CODE
N
Y
279
PROMPT FOR QUESTIONS/ANSWERS
281
WAIT FOR RESPONSE
283
PROMPT OPERATOR FOR USER CARD
285
ERASE USER CARD
287
WRITE INFO. TO USER CARD
WAIT FOR VALID ADMIN. CARD
289
291
GET AUTHORIZATION CODE FROM CARD
293
COMPARE CODE TO RESPONSE
295
CORRECT CODE
N
Y
297
PROMPT OPERATOR FOR USER CARD
299
INITIALIZE USER CARD
301
PROMPT OPERATOR TO REMOVE CARD
303
WAIT FOR USER CARD REMOVAL
305
LAST CARD
N
Y
END

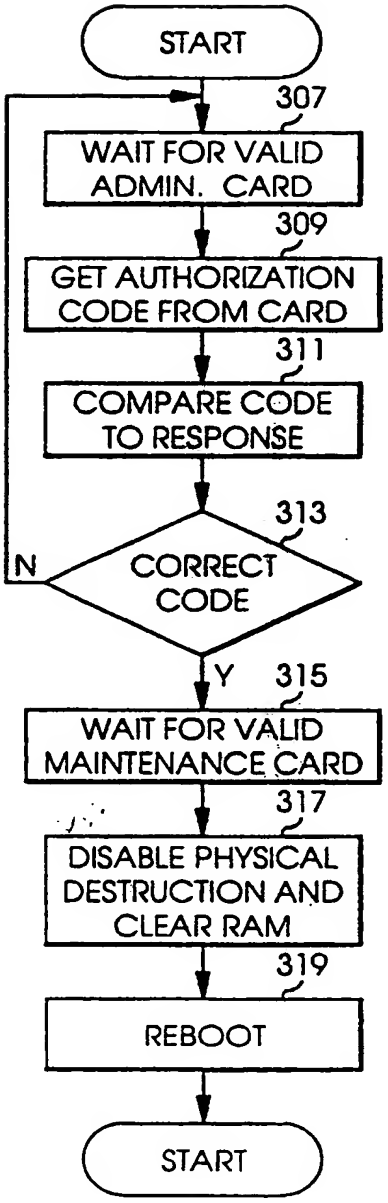

START
307
WAIT FOR VALID ADMIN. CARD
309
GET AUTHORIZATION CODE FROM CARD
311
COMPARE CODE TO RESPONSE
313
CORRECT CODE
N
Y
315
WAIT FOR VALID MAINTENANCE CARD
317
DISABLE PHYSICAL DESTRUCTION AND CLEAR RAM
319
REBOOT
START

*Fig. 7*

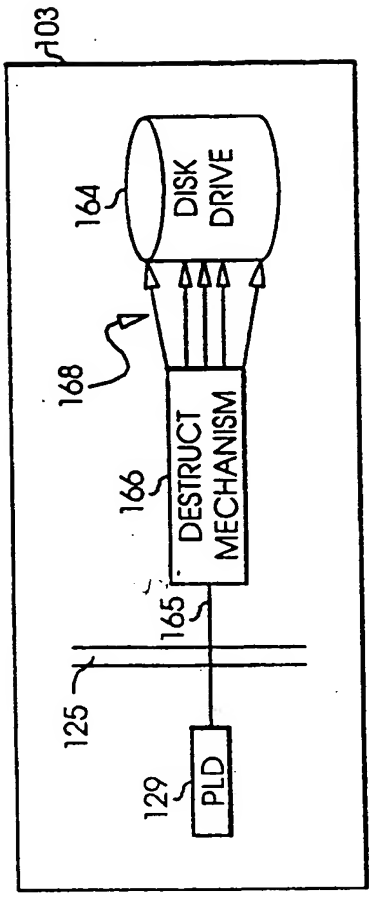

103
164
DISK DRIVE
168
166
DESTRUCT MECHANISM
165
125
129
PLD

Fig. 8

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 93/05357

A. CLASSIFICATION OF SUBJECT MATTER
IPC 5 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 5 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | EP,A,0 170 716 (TOSHIBA) 12 February 1986<br>see abstract | 1,2,4 |
| A | EP,A,0 458 614 (NEC CORPORATION) 22 May 1990<br>see abstract | 1,2,4 |
| A | GB,A,2 112 190 (OMRON TATEISI ELECTRONICS) 13 July 1983 | 1,2,4 |
| X | see page 2, line 63 - line 75<br>see page 3, line 52 - line 65<br>see line 85 - line 94<br>see claim 1 | 9,10 |

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 6 October 1993 | 18. 10. 93 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. ( + 31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax ( + 31-70) 340-3016 | TACCOEN, J |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 93/05357

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | FR,A,2 584 514 (CASIO COMPUTER CO) 9 January 1987<br>see abstract<br>see page 3, line 3 - line 13 | 1,2,4 |
| X | see claim 1 | 9,10 |
| A | EP,A,0 216 375 (CASIO COMPUTER COMPANY) 1 April 1987<br>see column 20, line 28 - column 21, line 41<br>see abstract | 1,2,4 |
| A | EP,A,0 262 025 (FUJITSU) 30 March 1988<br>see abstract | 1,2,4 |
| A | EP,A,0 182 244 (OKI ELECTRIC INDUSTRY COMPANY) 28 May 1986<br>see abstract<br>see page 28, line 28 - page 33, line 16<br>see claim 1 | 1,2,4 |
| A | EP,A,0 190 733 (TOSHIBA) 13 August 1986<br>see abstract<br>see page 4, line 22 - page 8, line 13 | 1,2,4 |
| A | GB,A,2 112 190 (OMRON TATEISI ELECTRONICS) 13 July 1983<br>see abstract | 1,2,4 |

| | | | | |
|---|---|---|---|---|
| EP-A-0170716 | 12-02-86 | US-A- | 4641374 | 03-02-87 |
| EP-A-0458614 | 27-11-91 | JP-A- | 4026990 | 30-01-92 |
| | | US-A- | 5208781 | 04-05-93 |
| GB-A-2112190 | 13-07-83 | JP-A- | 58132860 | 08-08-83 |
| | | JP-C- | 1733553 | 17-02-93 |
| | | JP-B- | 4011903 | 02-03-92 |
| | | JP-A- | 58109967 | 30-06-83 |
| | | JP-C- | 1643173 | 28-02-92 |
| | | JP-B- | 3006543 | 30-01-91 |
| | | JP-A- | 58109968 | 30-06-83 |
| | | DE-A,C | 3247846 | 07-07-83 |
| | | US-A- | 4528442 | 09-07-85 |
| FR-A-2584514 | 09-01-87 | JP-A- | 62009470 | 17-01-87 |
| | | DE-A,C | 3622257 | 15-01-87 |
| | | US-A- | 4801787 | 31-01-89 |
| EP-A-0216375 | 01-04-87 | JP-A- | 62072064 | 02-04-87 |
| | | JP-A- | 62072088 | 02-04-87 |
| | | US-A- | 4752677 | 21-06-88 |
| EP-A-0262025 | 30-03-88 | JP-A- | 63073348 | 02-04-88 |
| | | CA-A- | 1298653 | 07-04-92 |
| | | DE-A- | 3784824 | 22-04-93 |
| | | US-A- | 4853522 | 01-08-89 |
| EP-A-0182244 | 28-05-86 | JP-C- | 1760348 | 20-05-93 |
| | | JP-B- | 4048270 | 06-08-92 |
| | | JP-A- | 61166680 | 28-07-86 |
| | | JP-C- | 1751290 | 08-04-93 |
| | | JP-B- | 4038032 | 23-06-92 |
| | | JP-A- | 61114895 | 02-06-86 |
| | | JP-C- | 1712785 | 27-11-92 |
| | | JP-B- | 3076515 | 05-12-91 |
| | | JP-A- | 61121171 | 09-06-86 |
| | | JP-C- | 1751292 | 08-04-93 |
| | | JP-B- | 4038033 | 23-06-92 |
| | | JP-A- | 61125681 | 13-06-86 |

| | | | | |
|---|---|---|---|---|
| EP-A-0182244 | | JP-C- | 1712787 | 27-11-92 |
| | | JP-B- | 3076514 | 05-12-91 |
| | | JP-A- | 61127068 | 14-06-86 |
| | | US-A- | 4864109 | 05-09-89 |
| EP-A-0190733 | 13-08-86 | JP-A- | 61177585 | 09-08-86 |
| | | DE-A- | 3684932 | 27-05-92 |
| GB-A-2112190 | 13-07-83 | JP-A- | 58132860 | 08-08-83 |
| | | JP-C- | 1733553 | 17-02-93 |
| | | JP-B- | 4011903 | 02-03-92 |
| | | JP-A- | 58109967 | 30-06-83 |
| | | JP-C- | 1643173 | 28-02-92 |
| | | JP-B- | 3006543 | 30-01-91 |
| | | JP-A- | 58109968 | 30-06-83 |
| | | DE-A,C | 3247846 | 07-07-83 |
| | | US-A- | 4528442 | 09-07-85 |